ELSEVIER Discrete Mathematics 135 (1994) 69–79

DISCRETE MATHEMATICS

On exponentiation of G-sets☆

Andreas Blass

Mathematics Department, University of Michigan, Ann Arbor, MI 48109, USA

Received 26 March 1991

Abstract

We show that Joyal's rule of signs in combinatorics arises naturally from Dress's concept of exponentiation of virtual G-sets. We also show that two finite G-sets admit a G-equivariant bijection between their power sets if and only if the (complex) linear representations they determine are equivalent.

0. Introduction

We present in this paper two theorems about exponentiation of (actual or virtual) G-sets, where G is a finite group. The first theorem uses a special case of Dress's concept of exponentiation for virtual G-sets [2] to clarify the rule of signs introduced by Joyal [3, 4] in his theory of virtual species. The second relates the power sets of (actual) G-sets to the corresponding linear representations of G.

Section 1 is devoted to a review of the needed parts of the well-known theory of Burnside rings of finite groups, including Dress's exponentiation. Sections 2 and 3 contain the proofs of the two theorems and some additional remarks and examples.

1. Burnside rings and exponentiation

Let G be a finite group. By a G-set, we mean a finite set A equipped with a left action of G, which we write as $g(a)$ or simply as ga. If A and B are two G-sets, then so are the disjoint union $A+B$ with G acting on each summand separately, the cartesian product $A\times B$ with G acting componentwise, and the set B^A of functions from A to B with G acting by

$$(gf)(a)=g(f(g^{-1}a)).$$

☆Partially supported by NSF grant DMR-8801988.

SSDI 0012-365X(93)E0109-H

These three constructions respect isomorphism, so we obtain operations of addition, multiplication and exponentiation on the set $S(G)$ of isomorphism classes of G-sets. The addition and multiplication operations make $S(G)$ into a commutative semi-ring with additive cancellation, so the formal differences of elements of $S(G)$ form a commutative ring (with unity, given by the one-element G-set) called the *Burnside ring* $\Omega(G)$ of G. Ignoring the distinction between a G-set and its isomorphism class, one often refers to elements of $S(G)$ as (actual) G-sets and to elements of $\Omega(G)$ as *virtual G-sets*.

It is clear that exponentiation cannot be reasonably extended from $S(G)$ to all of $\Omega(G)$, not even when G is trivial for then $S(G)=\mathbb{N}$ and $\Omega(G)=\mathbb{Z}$. Nevertheless, Dress [2] showed that, with any fixed actual exponent A, B^A is an algebraic function of B (in the sense defined in [2]) and therefore extends naturally to virtual G-sets B. Thus, exponentiation makes sense in $\Omega(G)$ as long as the exponent is an actual G-set.

We shall need a convenient framework for computations in Burnside rings. Every G-set is the disjoint union of transitive G-sets called its orbits, and every transitive G-set is isomorphic to one of the form G/H (the set of left cosets gH, acted upon according to $g'(gH)=(g'g)H$) where H ranges over a system $K(G)$ of representatives of the conjugacy classes of subgroups of G. It follows that the additive structure of $S(G)$ (resp. $\Omega(G)$) is easily described as the free abelian semi-group (resp. group) generated by the orbits G/H with $H\in K(G)$. Unfortunately, in this description, multiplication looks rather complicated, since the product of two orbits can be a complicated sum of orbits. We therefore prefer to describe elements of $\Omega(G)$ by means of the marks defined by Burnside [1, Section 180] as follows. For any G-set A and any subgroup H of G, the *mark of H in A* is the number $\langle H, A\rangle$ of elements of A fixed by the action of H. It is clear that, with a fixed H, this defines a homomorphism of semi-rings $S(G)\to\mathbb{N}$, which determines a unique homomorphism of rings $\Omega(G)\to\mathbb{Z}$, still denoted by $\langle H, \_\rangle$. The mark $\langle H, A\rangle$ equals the number of G-equivariant (i.e. preserving the G-action) maps from G/H to A. (An H-fixed $a\in A$ yields the equivariant map sending each gH to $g(a)$; an equivariant map $f: G/H\to A$ yields an H-fixed element $f(1H)\in A$; and these constructions are inverse to each other.) Hence, conjugate subgroups have the same marks, so it is customary to consider marks $\langle H, A\rangle$ only for $H\in K(G)$.

The $\langle H, \_\rangle$'s for all $H\in K(G)$ are the components of a ring homomorphism $\Omega(G)\to\mathbb{Z}^k$, where k is the number of conjugacy classes of subgroups of G. This homomorphism is known to be one-to-one; since we shall need this fact, we sketch the proof for the sake of completeness. View the additive structure of $\Omega(G)$ as the free abelian group generated by the G/H with $H\in K(G)$. Now

$$\langle H_1, G/H_2\rangle=0 \quad \text{if } |H_1|>|H_2|$$

(or even if H_1 is conjugate to no subgroup of H_2) because the stabilizers of elements of G/H_2 are the conjugates of H_2. On the other hand, $\langle H, G/H\rangle\neq 0$ since H fixes $1H$ in G/H. (In fact, $\langle H, G/H\rangle$ is the index of H in its normalizer.) Thus, if we order the groups in $K(G)$ according to size, then the matrix representing our ring-homomorphism (in terms of the $\{G/H\}$ basis for $\Omega(G)$ and the standard basis for $\mathbb{Z}^k$) is triangular with non-zero diagonal entries. So the homomorphism is one-to-one.

We shall need the marks in B^A, which may be easily computed as follows. Suppose first that both A and B are actual G-sets and that H is a subgroup of G. Then

$$\langle H, B^A\rangle = \text{The number of } H\text{-equivariant functions } A \to B.$$

Let us write $A|H$ and $B|H$ for A and B viewed as H-sets by restricting the given G-actions to H. Furthermore, let us decompose A into H-orbits, $A=\sum_{i=1}^{r} H/K_i$ for certain subgroups K_i of H. Then an H-equivariant map $A\to B$ is determined by r H-equivariant maps $f_i: H/K_i \to B|H$. The number of choices for f_i is the mark (relative to H) of K_i in $B|H$, which is also the mark (relative to G) of K_i in B. Thus,

$$\langle H, B^A\rangle = \prod_{i=1}^{r} \langle K_i, B\rangle, \tag{1}$$

where $A|H=\sum_{i=1}^{r} H/K_i$. The K_i need not belong to $K(G)$ (even if they belonged to $K(H)$), so if one insists on considering marks only of groups in $K(G)$ then each K_i in (1) should be replaced by its conjugate in $K(G)$.

Equation (1), although established under the assumption that both A and B are actual G-sets, continues to hold when B is a virtual G-set because both sides are algebraic functions so Dress's theorem about unique extensions [2] applies.

The formula (1) simplifies greatly if the G-action on B is trivial, i.e. if $B=b\cdot 1$ in $\Omega(G)$ for some $b\in\mathbb{N}$ (or $b\in\mathbb{Z}$). Then $\langle K_i, B\rangle = b$ regardless of what K_i is, so

$$\langle H, (b\cdot 1)^A\rangle = b^r, \tag{2}$$

where r is the number of H-orbits in A.

We finish this section by recalling Burnside's lemma [1, Section 145]. The number of orbits in a G-set A is

$$\frac{1}{|G|}\sum_{g\in G} \langle (g), A\rangle,$$

where (g) is the cyclic subgroup generated by g.

2. Joyal's rule of signs

Polynomial formulas arising in enumerative combinatorics frequently have a (new) enumerative interpretation when the variables are allowed to take negative values. For a simple example, fix $k\in\mathbb{N}$ and consider the polynomial in n enumerating the

k-element subsets of an n-element set:

$$\binom{n}{k}=\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

If we allow n to take negative values $-m$, with $m\in\mathbb{N}$, this polynomial

$$\binom{-m}{k}=(-1)^k\frac{m(m+1)(m+2)\cdots(m+k+1)}{k!}$$

enumerates (except for the sign $(-1)^k$) the k-element subsets of m with repeated elements allowed in the subsets.

Joyal [3,4] provided a general framework for considering such phenomena (as well as more general ones). He considered functors F, from the category of sets into itself, that have the form

$$F(A)=\sum_{n\geqslant 0} A^n \underset{S_n}{\times} F_n. \tag{3}$$

Here S_n is the symmetric group on n objects, F_n is an S_n-set, A^n is the nth cartesian power of A with S_n acting by permuting the n components, and $\underset{S_n}{\times}$ means the set of S_n-orbits in the cartesian product. To visualize what (3) means, it is useful to decompose each F_n into its S_n-orbits, say S_n/H_i for certain subgroups $H_i\in K(S_n)$. Then

$$\begin{aligned} A^n \underset{S_n}{\times} F_n &\cong \sum_i A^n \underset{S_n}{\times} (S_n/H_i) \\ &\cong \sum_i (A^n/H_i), \end{aligned}$$

where A^n/H_i means that the set of H_i-orbits in A^n. (Recall that S_n and therefore the subgroup H_i act on A^n by permuting the n components.) The isomorphism in the last line displayed above is a consequence of the easily verified general fact that, for any group G, subgroup H, and G-set X, $X \underset{G}{\times} (G/H)\cong X/H$; every G-orbit in $X\times(G/H)$ intersects the 'column' $X\times\{1H\}$, which can be identified with X, in an H-orbit.

These considerations show that $F(A)$ in (3) is just the disjoint union of various A^n/H_i, for (possibly) different n's and subgroups $H_i\in K(S_n)$. A^n/H_i should be viewed as the set of n-element subsets of A (possibly with repeated elements) with some extra structure. For example, when $n=3$, $A^3/\{1\}$ is the set of ordered triples from A, A^3/S_3 is the set of unordered triples, A^3/(alternating group) is the set of cyclically ordered triples, and A^3/(subgroup of order 2) is the set of triples with a distinguished first element but no relative order of the other two elements.

Joyal considered the problem of extending functors F of the form (3) to negative values of A, i.e., to virtual sets. Of course, the values of F will then also be virtual sets, and there is a strong temptation to write

$$F(-A)=\sum_{n\geq 0}(-1)^n A^n \underset{S_n}{\times} F_n \tag{4}$$

$$=\sum_{n\,\text{even}} A^n \underset{S_n}{\times}{}^n F_n - \sum_{n\,\text{odd}} A^n \underset{S_n}{\times} F_n.$$

This is wrong. For example, if $F(A)=A^2/S_2$, the set of unordered pairs with repetition allowed, then (4) gives $F(-A)=F(A)$, whereas $F(-A)$ ought to be the set of unordered pairs *without repetition*, or in any case something enumerated by $n(n-1)/2$, not $n(n+1)/2$, since reversing the sign of n in the latter yields the former.

Motivated by desirable formal properties of the 'exponential' functor $\sum_{n\geq 0} A^n/S_n$, Joyal [3,4] found the right definition of $F(-A)$, his *rule of signs*:

$$F(-A)=\sum_{n\geq 0} A^n \underset{S_n}{\times} \varepsilon^n F_n, \tag{5}$$

where ε^n is the virtual S_n-set $\varepsilon_0^n-\varepsilon_1^n$ given by

$$\varepsilon_0^n=\{f \mid f \text{ maps } n \text{ onto an even } k\in\mathbb{N}\},$$

$$\varepsilon_1^n=\{f \mid f \text{ maps } n \text{ onto an odd } k\in\mathbb{N}\}.$$

(We use here the standard set-theoretic identification of a natural number n with the set $\{0,1,\dots,n-1\}$, and similarly for k.) S_n acts on ε_0^n and ε_1^n by permuting the domains of the f's.

Notice that, for the example $F(A)=A^2/S_2$ considered earlier, (5) gives

$$F(-A)=A^2 \underset{S_2}{\times} \varepsilon^2=(A^2 \underset{S_2}{\times} \varepsilon_0^2)-(A^2 \underset{S_2}{\times} \varepsilon_1^2).$$

ε_0^2 consists of the two surjections $2\to 2$, which S_2 interchanges, so $\varepsilon_0^2=S_2/\{1\}$ and therefore $A^2 \underset{S_n}{\times} \varepsilon_0^2=A^2/\{1\}=A^2$. ε_1^2 consists of the one surjection $2\to 1$, so $A^2 \underset{S_n}{\times} \varepsilon_1^2= A^2/S_2$. Thus, $F(-A)=A^2-(A^2/S_2)$. The enumerating function for this is $n^2-(n(n+1)/2)=n(n-1)/2$, as it should be.

We digress for a moment to answer a possible objection, namely that, although $F(-A)$ has the expected enumerating function $n(n-1)/2$, it is not the expected result, the set of unordered pairs from A without repetition. One answer is that this expected result is not a functor of A, as it does not transform reasonably under maps $A\to B$ that are not one-to-one. A better answer, using only bijective maps, can be obtained by considering what happens when A is not merely a set but a G-set for some non-trivial group G, say $G=S_2$ for simplicity. Then A consists of a number p of fixed points and a number of q of two-element orbits. An easy computation shows that $F(A)=A^2/S_2$ has

$$\frac{p(p+1)}{2}+q \text{ fixed points} \quad \text{and} \quad pq+q^2 \text{ two-element orbits.} \tag{6}$$

The ‘expected’ result, the set of unordered pairs without repetitions, has

$$\frac{p(p-1)}{2}+q \text{ fixed points} \quad \text{and} \quad pq+q(q-1) \text{ two-element orbits.}$$

which is *not* the result of reversing the signs of p and q in (6). On the other hand, since A^2 has

$$p^2 \text{ fixed points} \quad \text{and} \quad 2pq+2q^2 \text{ two-element orbits,}$$

we find, by subtracting (6), that $A^2-(A^2/S_2)$ has

$$\frac{p(p-1)}{2}-q \text{ fixed points} \quad \text{and} \quad pq+q^2 \text{ two-element orbits,}$$

which *is* the result of reversing the signs of p and q in (6). Thus, Joyal's formula for $F(-A)$ is (at least) more acceptable than the expected result.

We shall show that Joyal's rule of signs arises quite naturally from Dress's concept of exponentiation in Burnside rings. To see this, let us return to the formula (3) for $F(A)$ and consider how the S_n-action involved in it arises. F_n is given as an S_n-set, but S_n also acts on the other factor, A^n, by permutation of components. That is to say, what we have called A^n is actually the (exponential) S_n-set $(A\cdot 1)^{\underset{\sim}{n}}$ where $A\cdot 1$ is the set A with trivial S_n action while $\underset{\sim}{n}$ is the set $n=\{0,1,2,\ldots,n-1\}$ with the natural action of S_n on it. The distinction between the trivial S_n-set $A\cdot 1$ and the mere set A will be unimportant; we henceforth write simply A, and the trivial action is to be tacitly understood. The distinction between the *non-trivial* S_n-set $\underset{\sim}{n}$ and the mere set (or number) n, on the other hand, is crucial. In fact, this distinction is the source of the error in (4). Keeping track of the distinction, we find that the first line of (4) should read

$$F(-A)=\sum_{n\geqslant 0}(-1)^{\underset{\sim}{n}}A^{\underset{\sim}{n}}\underset{S_n}{\times}F_n,$$

and the second line of (4) is no longer justified since $(-1)^{\underset{\sim}{n}}$ is not merely ± 1 according as n is even or odd. In fact, in place of the second line of (4), we now get Joyal's rule of signs, by virtue of the following result.

Theorem 2.1. $(-1)^{\underset{\sim}{n}}=\varepsilon^n$, *as virtual* S_n*-sets.*

Proof. According to results in Section 1, it suffices to check that the marks $\langle H,(-1)^{\underset{\sim}{n}}\rangle$ and $\langle H,\varepsilon^n\rangle$ agree, for all subgroups H of S_n. By (2), $\langle H,(-1)^{\underset{\sim}{n}}\rangle=(-1)^r$, where r is the number of H-orbits in $\underset{\sim}{n}$. So it remains to calculate

$$\begin{aligned}\langle H,\varepsilon^n\rangle&=\langle H,\varepsilon_0^n\rangle-\langle H,\varepsilon_1^n\rangle\\&=\sum_k(-1)^k\cdot(\text{Number of } H\text{-fixed surjections } \underset{\sim}{n}\to k).\end{aligned}$$

Since H acts on the surjections by permuting the domains, a surjection is fixed by H if and only if it is constant on each of the r orbits of H in $\underset{\sim}{n}$. Viewing such a surjection as a function on the set of orbits, we have

$$\langle H, \varepsilon^n \rangle = \sum_k (-1)^k \cdot (\text{Number of surjections } r \to k).$$

The quickest way to compute this is to use the well-known polynomial identity

$$x^r = \sum_k S(r, k) \cdot x(x-1) \cdots (x-k+1),$$

where $S(r, k)$ is the Stirling number of the second kind, the number of partitions of r into k pieces. Putting $x = -1$, we find

$$\begin{aligned}(-1)^r &= \sum_k S(r, k) \cdot (-1)(-2) \cdots (-k) \\ &= \sum_k S(r, k)(-1)^k k!.\end{aligned}$$

Since $S(r, k)k!$ is the number of surjections $r \to k$, we have $\langle H, \varepsilon^n \rangle = (-1)^r = \langle H, (-1)^{\underset{\sim}{n}} \rangle$. $\square$

The crucial fact in the preceding proof, the identity

$$\sum_k (-1)^k. \ (\text{Number of surjections } r \to k) = (-1)^r \tag{7}$$

also has a bijective proof. The left side counts all surjections $f: r \to k$, for arbitrary k (necessarily $\leqslant r$), with weight $(-1)^k$. One of these surjections is the identity map $r \to r$, with weight $(-1)^r$, which matches the right side of (7). Thus, to prove (7) it suffices to pair off all the non-identity surjections f of positive weight with those of negative weight. Such a pairing $f \to f^*$ can be defined as follows. Given $f: r \to k$, not the identity map, view it as partitioning r into blocks $f^{-1}\{i\}$ for $i \in k$ and ordering the set of blocks according to the value of i. Let p be the smallest number $\in k$ such that $f^{-1}\{p\} \neq \{p\}$; this exists because f is not the identity. If p is the only element in its block, so $\{p\} = f^{-1}\{q\}$ for some $q > p$ (by choice of p), then we obtain f^* by merging this block with the previous one; that is,

$$f^*(x) = \begin{cases} f(x) & \text{if } f(x) < q, \\ f(x) - 1 & \text{if } f(x) \geqslant q. \end{cases}$$

If, on the other hand, p is not the only member of its block, so $\{p\} \subsetneq f^{-1}\{q\}$ for some $q \geqslant p$, then we split this block into $\{p\}$ and the rest, putting $\{p\}$ after the rest in the ordering; that is

$$f^*(x) = \begin{cases} f(x) & \text{if } f(x) \leqslant q \text{ and } x \neq p, \\ f(x) + 1 & \text{if } f(x) > q \text{ or } x = p. \end{cases}$$

In the first case, the range k decreases by 1, and in the second case it increases by 1, so the weight of f^* is always the negative of the weight of f. Furthermore, whichever case applies to f, the other applies to f^* with the same value of p, and $f^{**}=f$. So we have the desired pairing.

3. Linear representations and power sets

Any G-set A determines a (complex) linear representation $\mathbb{C}A$ of G; $\mathbb{C}A$ is the vector space of formal $\mathbb{C}$-linear combinations of elements of A, and G acts on it by the linear extension of its action on A. With respect to the basis A of $\mathbb{C}A$, the matrices of the representation of G are permutation matrices, and their traces, the characters of the representation, are given by the numbers of fixed points:

$$\chi_{\mathbb{C}A}(g) = \text{Number of points in } A \text{ fixed by } g = \langle (g), A \rangle.$$

It is entirely possible for two non-isomorphic G-sets to produce the same character and therefore isomorphic linear representations. All that is needed is for all the cyclic subgroups of G, but not all the non-cyclic subgroups of G, to have the same marks in the two G-sets, and this situation arises for every non-cyclic G. To see this, recall from Section 1 that $\Omega(G)$ is, in its additive structure, a free abelian group of rank equal to the number k of conjugacy classes of subgroups of G, and that the marks define an embedding of $\Omega(G)$ into $\mathbb{Z}^k$. It follows easily that the marks of a proper subfamily of the subgroups in $K(G)$ cannot determine the other marks; in particular, the marks of cyclic subgroups do not determine the marks of non-cyclic subgroups.

We shall need to refer to the examples of this phenomenon involving the two smallest non-cyclic groups, so we describe these examples here. (A more complicated example given by Burnside [1, Section 217] can be described as follows. The set X of points and the set Y of lines in the projective plane of seven points (over the field $\mathbb{Z}_2$) are non-isomorphic G-sets, where G is this plane's collineation group (of order 168), but $\mathbb{C}X$ and $\mathbb{C}Y$ are isomorphic linear representations of G. Unlike the examples that follow, this one involves transitive G-sets.)

If G is the Klein four-group $V=\{1,a,b,c\}$, we define A to be the transitive V-set $V/(a)$, and similarly for B and C. In addition to these three V-orbits, there are the regular action $V=V/(1)$ and the trivial one-element V-set $1=V/V$. By inspection of the characters, one finds that the V-sets $A+B+C$ and $V+1+1$ determine isomorphic linear representations.

If G is the symmetric group S_3, there are four non-isomorphic transitive actions: the regular action $S_3=S_3/(1)$, the natural action $\underset{\sim}{3}=S_3/(t)$ where t is any one of the three transpositions, the two-element G-set $A=S_3/(c)$ where c is a 3-cycle (so (c) is the alternating group), and the trivial action $1=S_3/S_3$. By inspection of characters again, one finds that the S_3-sets $\underset{\sim}{3}+\underset{\sim}{3}+A$ and S_3+1+1 determine isomorphic linear representations.

The main result of this section was suggested when Norbert Brunner remarked to me that the Klein four-group V has two non-isomorphic V-sets whose power sets are isomorphic. (Brunner cites [5] as the source of this observation.) It turned out that the two V-sets he had in mind were the same two, $A+B+C$ and $V+1+1$, as in the first example above. This is no coincidence.

Theorem 3.1. *For any two G-sets A and B, the following are equivalent.*

(a) *$\mathbb{C}A$ and $\mathbb{C}B$ are equivalent representations of G.*

(b) *2^A and 2^B are isomorphic G-sets. (Here 2 is a two-element set with trivial G-action, so 2^A is the power set of A.)*

(c) *$\mathbb{C}2^A$ and $\mathbb{C}2^A$ are equivalent representations of G.*

Proof. Consider the data needed to determine $\mathbb{C}A$, 2^A, and $\mathbb{C}2^A$ (up to G-isomorphism for 2^A, and up to linear G-isomorphism in the other two cases). For $\mathbb{C}A$, we need the characters, i.e. the marks $\langle (g), A\rangle$ of cyclic subgroups in A. For 2^A, we need the marks $\langle H, 2^A\rangle$ of all subgroups H in 2^A. For $\mathbb{C}2^A$, we need the marks $\langle (g), 2^A\rangle$ of cyclic subgroups in 2^A. So the theorem will be established if we show that all marks in 2^A are determined by the cyclic marks in A and that the cyclic marks in A are determined by the cyclic marks in 2^A.

For the first of these, we need only recall from Section 1 that

$$\langle H, 2^A\rangle = 2^r,$$

where r is the number of H-orbits in A, and that, by Burnside's lemma,

$$r = \frac{1}{|H|} \sum_{g\in H} \langle (g), A\rangle.$$

So the cyclic marks in A suffice to determine all the marks in 2^A, as desired.

For the second objective, suppose that we are given the cyclic marks $\langle (h), 2^A\rangle$; we seek to determine the cyclic marks $\langle (g), A\rangle$. As above, they are related by

$$\log_2 \langle (h), 2^A\rangle = \frac{1}{|(h)|} \sum_{g\in (h)} \langle (g), A\rangle.$$

This system of equations expresses the known quantities on the left as linear combinations of unknown marks on the right. The matrix of this linear system is triangular with non-zero diagonal entries if we order the cyclic groups consistently with their sizes; indeed, in the equation with (h) on the left, the subgroups (g) that appear on the right are (h) and smaller subgroups. Therefore, the matrix is invertible, which means that we can express the desired quantities $\langle (g), A\rangle$ as (rational) linear combinations of the known quantities $\log_2 \langle (h), 2^A\rangle$. $\square$

Theorem 3.1 establishes a connection between the linearizations $\mathbb{C}A$ and the power sets 2^A of G-sets A. The existence of such a connection may seem less surprising if one remembers that the power set (of a finite set) is itself a sort of linearization; specifically,

2^A is the underlying set of the vector space $\mathbb{Z}_2 A$ with basis A over the two-element field $\mathbb{Z}_2$. This point of view would lead one to suspect that the equivalent conditions in Theorem 2 should also be equivalent to the following, which can be viewed as a '$\mathbb{Z}_2$ version' of (a) or as a 'linear version' of (b):

(d) $\mathbb{Z}_2 A$ and $\mathbb{Z}_2 B$ are equivalent $\mathbb{Z}_2$-representations of G.

But things are not so simple. Of course (d) implies (b) (hence (a) and (c)) because (d) requires a $\mathbb{Z}_2$-linear G-isomorphism where (b) requires only a G-bijection. But here is a counter example to the converse implication.

Let G be the Klein four-group V, and consider the V-sets $A+B+C$ and $V+1+1$. We have already observed that these satisfy condition (a) of Theorem 2, hence also conditions (b) and (c). But they do not satisfy (d). One way to see this is to consider, in each of $\mathbb{Z}_2(A+B+C)$ and $\mathbb{Z}_2(V+1+1)$, the vectors that are fixed by at least one non-identity element in V. In $\mathbb{Z}_2(A+B+C)$, these vectors include the six standard basis vectors (as both elements of A are fixed by $a \in V$, and similarly for B and C), so they span the entire space. In $\mathbb{Z}_2(V+1+1)$, on the other hand, these vectors all have the property that the sum of the coefficients of the basis vectors in V is zero (in $\mathbb{Z}_2$) — i.e., every subset of $V+1+1$ with non-trivial stabilizer contains an even number of points from the orbit V — so they do not span the whole space. (It can be shown that, if G is a p-group and X and Y are G-sets with $\mathbb{Z}_p X \cong \mathbb{Z}_p Y$ as linear representations of G over $\mathbb{Z}_p$, then $X \cong Y$ as G-sets. This subsumes what we have just shown as well as the following sentence.)

The preceding argument can be extended to show that non-isomorphic V-sets never generate isomorphic $\mathbb{Z}_2$-linear representations. But this fact about V does not extend to arbitrary groups. Specifically, the non-isomorphic S_3-sets $\underset{\sim}{3}+\underset{\sim}{3}+A$ and S_3+1+1 generate S_3-isomorphic $\mathbb{Z}_2$-linear spaces. Here is an easy way to see the linear isomorphism. In the two-dimensional affine space over the field $\mathbb{Z}_3$ (where there are nine points and 12 lines), fix a point O, and consider the configuration consisting of the set X of the eight points other than O and the set Y of the eight lines not passing through O. The linear transformation $f : \mathbb{Z}_2 Y \to \mathbb{Z}_2 X$ that sends each line $\in Y$ to the sum of the three points on it is a surjection, because each point $P \in X$ is f of the sum of the three lines through P and the two lines parallel to OP. So f is an isomorphism. It clearly commutes with the natural actions on X and Y of any group of affine transformations that fix O. Choose a point $P \neq O$, and consider the group of affine motions that fix both O and P (and therefore also the third point Q of line OP). This group is isomorphic to S_3. Its action on X is isomorphic to S_3+1+1, the two fixed points $(1+1)$ being P and Q. Its action on Y is isomorphic to $\underset{\sim}{3}+\underset{\sim}{3}+A$, where one copy of $\underset{\sim}{3}$ consists of the lines through P, the other of the lines through Q, and A of the lines parallel to OPQ.

References

[1] W. Burnside, Theory of Groups of Finite Order (Cambridge University Press, Cambridge, 2nd ed., 1911) (reprinted by Dover, New York, 1955).

[2] A. Dress, Operations in representation rings, in: I. Reiner, ed., Representation Theory of Finite Groups and Related Topics; Proc. Symp. Pure Math. Vol. XXI, Amer. Math. Soc. (1971) 39–45.
[3] A. Joyal, Règle des signes en algèbre combinatoire, C.R. Math. Acad. Sci. Canada 7 (1985) 285–290.
[4] A. Joyal, Foncteurs analytiques et espèces de structures, in: G. Labelle and P. Leroux, eds., Combinatoire énumérative, Lecture Notes in Math., Vol. 1234 (Springer, Berlin, 1986) 126–159.
[5] H. Läuchli, Auswahlaxiom in der Algebra, Comm. Math. Helv. 37 (1962) 1–18.